Model Theory

Ivan Tomašić

LTCC 2009

Outline

Contents

1 First order logic

Languages

A *language* is a triple $\mathcal{L}$ which consists of:

- a set of function symbols $\{f_i : i \in I_0\}$ (where each f_i is of some arity n_i);
- a set of relation symbols $\{R_i : i \in I_1\}$ (where each R_i is of some arity m_i);
- a set of constant symbols $\{c_i : i \in I_2\}$.

Any of I_0, I_1, I_2 can be empty.

Formulae

Given a language $\mathcal{L}$, a *first-order* $\mathcal{L}$*-formula* is any 'meaningful' *finite* string of symbols made out of

- symbols from $\mathcal{L}$;
- equality symbol $=$;
- variables $x_0, x_1, x_2, \ldots$;
- logical connectives $\neg$, $\wedge$, $\vee$;
- quantifiers $\exists$, $\forall$;
- parentheses.

I trust you are experienced enough to be able to recognise what makes a formula *'meaningful'*.

Example: formulae in the language of groups

Let $\mathcal{L}$ be the language consisting of a single binary function (operation) '$\cdot$'. Valid $\mathcal{L}$-formulae include:

- $\exists x_0 \forall x_1 \;\; x_0 \cdot x_1 = x_1 \wedge x_1 \cdot x_0 = x_1$.
- $\forall x_1 \;\; x_0 \cdot x_1 = x_1 \cdot x_0$.

Example: formulae in the language of groups

Although $\mathcal{L}$ is enough for expressing all properties of groups, it is more economical to formulate group-theoretic discussions in the language $\mathcal{L}_g$ consisting of a binary operation $\cdot$, unary operation $^{-1}$ and a constant e. We may write:

- $\forall x_1 \;\; x_1 \cdot e = x_1 \wedge e \cdot x_1 = x_1$;
- $\forall x_1 \;\; x_1 \cdot x_1^{-1} = e \wedge x_1^{-1} \cdot x_1 = e$;
- $\exists x_1 \exists x_2 \;\; x_0 = x_1 \cdot x_2 \cdot x_1^{-1} \cdot x_2^{-1}$.

Example: formulae in the language of ordered rings

Let $\mathcal{L}_{or}$ be the language consisting of binary functions $+, \cdot$, a binary relation $<$ and constant symbols 0, 1. Valid $\mathcal{L}_{or}$-formulae include:

- $x_1 = 0 \vee (\neg(x_1 < 0))$;
- $\exists x_2 \;\;\; x_2 \cdot x_2 = x_1$;
- $\forall x_1 (x_1 = 0 \vee \exists x_2 \;\; x_2 \cdot x_1 = 1)$;
- $x_1^2 + x_2^2 \leq 1 + 1 + 1 + 1$.

What is a fundamental difference between the second and the third formula?

Free and bound variables

- A variable is *bound* in a formula if it is in the scope of a quantifier, otherwise it is *free*.
- If variables $x_1, \ldots, x_n$ occur freely in a formula φ, we often express it by writing $\varphi(x_1, \ldots, x_n)$.
- A formula with no free variables is called a *sentence*.

Exercise: which variables are free, and which are bound in the examples above? Which formulae are sentences?

Structures

Given a language $\mathcal{L} = (\{f_i\}, \{R_i\}, \{c_i\})$, an $\mathcal{L}$-*structure* is a set M in which each symbol from $\mathcal{L}$ is assigned an interpretation. In particular:

- for each n_i-ary function symbol f_i, we are given a function $f_i : M^{n_i} \to M$ (abuse of language, we should really write $f_i^M : M^{n_i} \to M$);
- for each m_i-ary relation symbol R_i, we are given a relation $R_i \subseteq M^{m_i}$;
- for each constant symbol c_i, we are given an element $c_i \in M$.

Morphisms of structures

- A map $f : M \to N$ between two $\mathcal{L}$-structures is a *homomorphism*, if
  - for each function symbol F of $\mathcal{L}$ of arity n, $f \circ F^M = F^N \circ f^n$;
  - for each relation symbol R of $\mathcal{L}$ of arity m, $f(R^M) \subseteq R^N$;
  - for each constant c of $\mathcal{L}$, $f(c^M) = c^N$.
- An injective homomorphism is called an *embedding* if in addition $f(R^M) = R^N \cap f(M^m)$ for each relation symbol.
- An *isomorphism* is a surjective embedding $f : M \to N$. Write $M \cong N$ when isomorphic.

Substructures

- Given two $\mathcal{L}$-structures M and N with $N \subseteq M$, we say that N is a *substructure* of M if the inclusion $N \to M$ is an embedding.
- By abuse of notation, we write $N \subseteq M$ to express that N is a substructure of M.

Satisfaction, realisation

- Let M be an $\mathcal{L}$-structure, $\varphi(x_1, \ldots, x_n)$ an $\mathcal{L}$-formula, and let $a_1, \ldots, a_n \in M$. We say that M *satisfies* $\varphi(a_1, \ldots, a_n)$ and write

  $$M \models \varphi(a_1, \ldots, a_n),$$

  if the property expressed by φ is true for $a_1, \ldots a_n$ within M (all quantifiers are interpreted as ranging over M).
- The *set of realisations* of $\varphi(x_1, \ldots, x_n)$ in M is the set

  $$\varphi(M) = \{(a_1, \ldots, a_n) \in M^n \quad : \quad M \models \varphi(a_1, \ldots, a_n)\}.$$

- NB: if φ is a sentence, it is either true or false in a given M.

Example: satisfaction

We consider $(\mathbb{N}, +, id, 0)$ and $(\mathbb{Z}, +, x \mapsto -x, 0)$ as $\mathcal{L}_g = (\cdot, ^{-1}, e)$-structures. Let φ be the sentence $\forall x_1 \exists x_2 \ \ x_1 \cdot x_2 = e$. Then clearly

- $\mathbb{N} \not\models \varphi$, while
- $\mathbb{Z} \models \varphi$.

Example: realisations

Consider the formulae $\varphi(x_1) \equiv \exists x_2 \ \ x_1 = x_2 \cdot x_2$, $\varphi_4(x_5) \equiv \exists x_1 \exists x_2 \exists x_3 \exists x_4 \ \ x_5 = x_1 \cdot x_1 + x_2 \cdot x_2 + x_3 \cdot x_3 + x_4 \cdot x_4$, $\psi(x_1, x_2) \equiv x_1 \cdot x_1 + x_2 \cdot x_2 = 1$ in the language $\mathcal{L}_r = (+, \cdot, 0, 1)$ of rings.

Then:

- $\varphi(\mathbb{R}) = \mathbb{R}_0^+$;
- $\varphi(\mathbb{C}) = \mathbb{C}$;
- $\psi(\mathbb{R})$ is the unit circle in the 'plane' $\mathbb{R}^2$;
- $\varphi_4(\mathbb{Z}) = \mathbb{N}$ (by Lagrange's four square theorem!!!).

Definable sets

We say that a set $X \subseteq M^n$ is *definable* (with parameters from a subset $B \subseteq M$) if there is a formula $\varphi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ and $b_1, \ldots, b_m \in B$ such that

$$X = \varphi(M, \bar{b}) := \{(a_1, \ldots, a_n) \ : \ M \models \varphi(a_1, \ldots, a_n, b_1, \ldots, b_m)\}.$$

Example: definability with and without parameters

Thinking of $\mathbb{R}$ as an ordered ring, the set $\{x : x > \sqrt{2}\}$ is definable with no parameters by a formula $\varphi(x) \equiv 1 + 1 < x \cdot x$. On the other hand, in order to define $\{x : x > \pi\}$, we need the parameter π.

Limitations of first order logic

We can only quantify over *elements* of a structure, not over subsets, functions or even natural numbers if they are not part of the structure.

For example, we *cannot*:

- express that a group is torsion;
- express that a graph is connected;
- characterise $\mathbb{R}$ up to isomorphism (the Archimedean axiom is not first order);
- state that a ring is a PID, etc.

Elementary equivalence

- Two $\mathcal{L}$-structures M and N are *elementarily equivalent*, written $M \equiv N$, if for every $\mathcal{L}$-sentence φ,

$$M \models \varphi \text{ if and only if } N \models \varphi.$$

- An $\mathcal{L}$-embedding $f : M \to N$ is *elementary* if for all $a_1, \ldots, a_n \in M$ and for any formula $\varphi(x_1, \ldots, x_n)$,

$$M \models \varphi(a_1, \ldots, a_n) \text{ if and only if } N \models \varphi(f(a_1), \ldots, f(a_n)).$$

  In other words, f preserves all formulae.

- If M is a substructure of N, we say that M is an *elementary substructure* if the inclusion map is elementary. Write $M \preceq N$.

Example: non-elementary substructure

In the previous example, $\mathbb{R}$ is a substructure of $\mathbb{C}$, but $\varphi(\mathbb{R}) = \mathbb{R}_0^+$ and $\varphi(\mathbb{C}) = \mathbb{C}$ so

$$\varphi(\mathbb{R}) \neq \varphi(\mathbb{C}) \cap \mathbb{R}.$$

Thus $\mathbb{R} \not\preceq \mathbb{C}$.

Aside: a categorical point of view

Let $\mathcal{S}_\mathcal{L}$ be the category of $\mathcal{L}$-structures with elementary embeddings as morphisms. A formula $\varphi(\bar{x})$ can be identified with its realisation functor $F_\varphi : \mathcal{S}_\mathcal{L} \to Set$,

$$F_\varphi(M) = \varphi(M).$$

An implication $\varphi \to \psi$ induces a natural transformation $F_\varphi \to F_\psi$.

Elementary equivalence vs isomorphism

Theorem 1. *If M and N are isomorphic, then they are elementarily equivalent.*

Proof. In fact we show that an isomorphism $f : M \to N$ is an elementary embedding. This is done by induction on the complexity of formulae. □

Converse? Note $N \prec M$ implies $N \equiv M$, so the converse is false if we can find a proper elementary substructure.

Theories

- A *theory* in a language $\mathcal{L}$ is a set of $\mathcal{L}$-sentences (may be infinite).

- If T is a theory in a language $\mathcal{L}$, and M is an $\mathcal{L}$-structure, we say that M is a *model* of T, or that M models T, writing $M \models T$, if for every $\varphi \in T$, $M \models \varphi$.

- We say that φ is a *logical consequence* of T, $T \models \varphi$, if for every model M of T, $M \models \varphi$.
- We say that T *proves* φ, $T \vdash \varphi$, if there is a formal proof of the sentence φ starting from assumptions T.
- We say that T is *consistent* if it does not prove a contradiction.

Example: theory of groups

1. $\forall x \forall y \forall z\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$;
2. $\forall x\ x \cdot 1 = x$;
3. $\forall x\ x \cdot x^{-1} = 1$.

Models?

Example: theory of dense linear orders without endpoints

1. $\forall x\ x \not< x$;
2. $\forall x \forall y (x = y \vee x < y \vee y < x)$;
3. $\forall x \forall y \forall z (x < y \wedge y < z \rightarrow x < z)$;
4. $\forall x \forall y (x < y \rightarrow \exists z (x < z \wedge z < y))$;
5. $\forall x \exists z\ z < x$; $\forall x \exists z\ x < z$.

Example: theory of algebraically closed fields

- the usual algebraic axioms for a field;
- axiom schema: for every n, add the axiom:

$$\forall y_0 \forall y_1 \cdots \forall y_{n-1} \exists x \quad y_0 + y_1 \cdot x + \cdots + y_{n-1} x^{n-1} + x^n = 0,$$

  where we have used the notation x^k as a shorthand for $x \cdot x \cdot \ldots \cdot x$ (k times).

Thus, we need infinitely many axioms to state that a field is algebraically closed.

Example: Peano axioms

1. $\forall x\ x + 1 \neq 0$;
2. $\forall x \forall y (x + 1 = y + 1 \rightarrow x = y)$;
3. $\forall x\ x + 0 = x$; $\forall x \forall y\ \ x + (y + 1) = (x + y) + 1$;
4. $\forall x\ x \cdot 0 = 0$; $\forall x \forall y\ x \cdot (y + 1) = x \cdot y + x$;
5. $\forall x \neg (x < 0)$; $\forall x \forall y (x < (y + 1) \leftrightarrow x < y \vee x = y)$;
6. axiom schema: for each first-order formula $\varphi(x, \bar{z})$, have the axiom:

$$\forall \bar{z} (\varphi(0, \bar{z}) \wedge \forall x (\varphi(x, \bar{z} \rightarrow \varphi(x + 1, \bar{z})) \rightarrow \forall x \varphi(x, \bar{z})).$$

Completeness

Theorem 2 (Gödel's Completeness I)**.**

$$T \models \varphi \textit{ if and only if } T \vdash \varphi.$$

Theorem 3 (Completeness II)**.**

$$T \textit{ has a model if and only if } T \textit{ is consistent.}$$

Compactness

Easy consequence of the above:

Theorem 4 (Compactness Theorem)**.** *If every finite subset of T has a model, then T has a model.*

This is one the most fundamental tools of model theory.

Proof. If T has no model then, by Completeness II, T is inconsistent, i.e., there is a proof of a contradiction from T. Since proofs are finite sequences of statements, it can use only a finite number of assumptions from T so there is a finite inconsistent subset of T, which has no model by Completeness II. □

Complete theories

Definition 5. An $\mathcal{L}$-theory T is *complete* if for every $\mathcal{L}$-sentence φ, either $T \models \varphi$ or $T \models \neg\varphi$.

Equivalently, a theory is complete if any two of its models are elementarily equivalent.

The easiest way of producing a complete theory is, given a structure M, to consider the *complete theory* of M,

$$\mathrm{Th}(M) = \{\varphi \,:\, M \models \varphi\}.$$

Examples: (in)complete theories

1. The theory of groups is not complete. Why? Groups can be commutative and noncommutative.

2. The theory of algebraically closed fields in not complete. It does not decide the characteristic.

3. The theory of algebraically closed fields of fixed characteristic is complete. Proof next time.

4. The theory of dense linear orders without endpoints is complete. Proof next time.

Gödel's Incompleteness

Peano axioms are not complete and cannot be completed in a reasonable way.

Theorem 6 (Gödel's 1st Incompleteness Theorem)**.** *For every consistent theory 'containing' enough arithmetic, there is a statement which is true, but not provable in the theory.*

Idea of proof comes from the liar paradox, the sentence φ states: 'φ cannot be proved in T.

2 Basic model theory

Size of models

Question: given a consistent theory T, for which cardinals κ can we find models of size κ?

Löwenheim-Skolem Theorem(s)

Theorem 7 (down and up Löwenheim-Skolem)**.** *Let $\mathcal{L}$ be a language.*

- *Let M be an $\mathcal{L}$-structure and $X \subseteq M$. Then there exists $M_0 \preceq M$ such that $X \subseteq M_0$ and $|M_0| \leq |X| + |\mathcal{L}|$.*
- *Let M be an infinite $\mathcal{L}$-structure. Then for any cardinal $\kappa > |M|$, M has an elementary extension of cardinality κ.*

In particular:

Theorem 8. *If T is a countable theory with an infinite model, then T has models in all infinite cardinalities.*

Categoricity

Definition 9. We say that a theory T is *categorical* in an infinite cardinality κ, if T has, up to isomorphism, a unique model of cardinality κ. We also say that T is κ-*categorical*.

Vaught's test

Theorem 10 (Vaught's test)**.** *If all models of T are infinite and T is categorical in some infinite cardinality κ, then T is complete.*

Proof. Suppose T is not complete. Then there exists a sentence φ such that both $T \cup \{\varphi\}$ and $T \cup \{\neg\varphi\}$ are consistent. By Löwenheim-Skolem, we can find structures M and N of cardinality κ such that $M \models T \cup \{\varphi\}$ and $N \models T \cup \{\neg\varphi\}$.

This is impossible, as M must be isomorphic to N. $\square$

Theory of algebraically closed fields of fixed characteristic

For a prime number p, let ψ_p be the sentence

$$\forall x \quad \underbrace{x + x + \cdots + x}_{p \text{ times}} = 0.$$

- Let ACF_p be the theory of algebraically closed fields given earlier, together with ψ_p.
- Let ACF_0 be the theory of algebraically closed fields together with $\{\neg\psi_p : p \text{ prime}\}$.

Categoricity of ACF_p

Let us fix p a prime or 0 and an uncountable cardinal κ. Take two algebraically closed fields K_1 and K_2 of characteristic p and cardinality κ with transcendence bases S_1 and S_2. Since K_i is the algebraic closure of $k(S_i)$, (where the prime subfield k is either $\mathbb{F}_p$ of $\mathbb{Q}$), it follows that $|K_i| = |S_i| + \aleph_0$, so $|S_1| = |S_2|$. Pick any bijection $f : S_1 \to S_2$. It uniquely extends to an isomorphism $f : k(S_1) \to k(S_2)$, and, by the uniqueness of algebraic closure (up to isomorphism), we can find an isomorphism $K_1 \to K_2$.

Categoricity and completeness of ACF_p

Theorem 11. ACF_p *is κ-categorical for every uncountable κ.*

By Vaught's test, we get:

Corollary 12. ACF_p *is complete ($p \geq 0$).*

Categoricity of dense linear orders without endpoints

Theorem 13 (Cantor)**.** *If A and B are countable dense linear orders without endpoints, then $A \cong B$.*

Proof. Back and forth argument. Suppose we have a partial order-preserving bijection $f : A_0 \to B_0$, A_0 finite subset of A, B_0 finite subset of B. In the 'forth' direction, it is clearly possible, given $a \in A \setminus A_0$ to find some $b \in B \setminus B_0$ such that $f \cup \{(a, b)\}$ is again a partial order-preserving bijection. In the 'back' direction, given $b \in B \setminus B_0$, we can find $a \in A \setminus A_0$ such that $f \cup \{(a, b)\}$ is again a partial order-preserving bijection.

Enumerate A as a_i, $i \in \omega$, and B as b_i. We inductively form a sequence $f_j : A_j \to B_j$ of order-preserving partial bijections such that for every i, $a_i \in A_{2i} = \mathrm{Dom}\, f_{2i}$ and $b_i \in B_{2i+1} = \mathrm{Im}\, f_{2i+1}$.

The map $\cup_j f_j$ is clearly an isomorphism. $\square$

Categoricity and completeness of dense linear orders without endpoints

Cantor's theorem in model-theoretic terms states that the theory of dense linear orders without endpoints is $\aleph_0$-categorical.

By Vaught's test, we get:

Corollary 14. *The theory of dense linear orders without endpoints is complete.*

A remark and a question

NB some of the back-and-forth machinery is disguised in the proof of uniqueness of the algebraic closure (up to isomorphism).

A question for you:

- Is ACF_p $\aleph_0$-categorical?
- Is the theory of DLO without endpoints uncountably categorical?

Decidability

A theory T is *decidable* if there is an algorithm which determines for each sentence φ whether $T \models \varphi$.

Theorem 15. *A complete recursively enumerable theory is decidable.*

Proof. By completeness of T and the Completeness Theorem, there is either a proof of φ from T or a proof of $\neg\varphi$ from T. Thus we can systematically search through all finite strings of symbols until we find a proof of either φ or $\neg\varphi$. $\square$

Corollary 16. *The theory ACF_p is decidable for each $p \geq 0$.*

The Lefschetz principle

Theorem 17. *Let φ be a sentence in the language of rings. TFAE:*

1. *φ is true in $\mathbb{C}$.*
2. *φ is true in every algebraically closed field of char 0.*
3. *φ is true in some algebraically closed field of char 0.*
4. *There are arbitrarily large primes p such that φ is true in some algebraically closed field of char p.*
5. *There is an m such that for all $p > m$, φ is true in all algebraically closed fields of characteristic p.*

Proof of the Lefschetz principle

The equivalence of 1–3 is just the completeness of ACF_0 and $5 \Rightarrow 4$ is obvious.

For $2 \Rightarrow 5$, suppose $\mathrm{ACF}_0 \models \varphi$. By the completeness theorem, $\mathrm{ACF}_0 \vdash \varphi$ and the proof uses only finitely many $\neg\psi_p$. Thus, for large enough p, $\mathrm{ACF}_p \models \varphi$.

For $4 \Rightarrow 2$, suppose $\mathrm{ACF}_0 \not\models \varphi$. By completeness $\mathrm{ACF}_0 \models \neg\varphi$. By the above argument, $\mathrm{ACF}_p \models \neg\varphi$ so 4 fails.

Theorem of Ax

A striking application of the Lefschetz principle:

Theorem 18 (Ax). *Let $f : \mathbb{C}^n \to \mathbb{C}^n$ be an injective polynomial map. Then f is surjective.*

Proof. Let $f(\bar{x}) = (f_1(\bar{x}), \ldots, f_n(\bar{x}))$ and suppose $f_i \in \mathbb{C}[\bar{x}]$ are of total degrees less than some d. Let $\Phi_{n,d}$ be the first order sentence stating that every injective polynomial map in n coordinates whose coordinate functions are of degree at most d is surjective.

Clearly, if k is any finite field, $k \models \Phi_{n,d}$, and the same is true for any increasing union of finite fields. In particular, the algebraic closure of any finite field satisfies $\Phi_{n,d}$ and the Lefschetz principle implies that $\Phi_{n,d}$ also holds for $\mathbb{C}$. $\square$

Types

Let M be an $\mathcal{L}$-structure and let $A \subseteq M$. Let $\mathcal{L}_A$ be the language obtained by adding to $\mathcal{L}$ the constant symbols for all elements of A. Let $\mathrm{Th}_A(M)$ be the set of all $\mathcal{L}_A$-sentences true in M.

Definition 19.

- An *n-type over A* is a set of $\mathcal{L}_A$-formulae in free variables $x_1, \ldots, x_n$ that is consistent with $\mathrm{Th}_A(M)$.
- An n-type p over A is *complete* if for every $\mathcal{L}_A$-formula $\varphi(\bar{x})$, either $\varphi(\bar{x}) \in p$ or $\neg\varphi(\bar{x}) \in p$.
- Incomplete types are sometimes called *partial*.
- Let $S_n(A)$ denote the set of all complete n-types over A.

Types and realisations

An easy way of producing a complete type: Let N be an elementary extension of M and let $\bar{b} \in N^n$. Then

$$tp(\bar{b}/A) := \{\varphi(\bar{x}) \in \mathcal{L}_A \ : \ N \models \varphi(\bar{b})\}$$

is a complete type.

On the other hand, if we have a partial n-type over A, it will be realised in some elementary extension N of M.

Types and automorphisms

Theorem 20. *Let $\bar{a}, \bar{b} \in M^n$ and $tp(\bar{a}/A) = tp(\bar{b}/A)$. Then there is an elementary extension N of M and an $\mathcal{L}$-automorphism of N fixing A and mapping $\bar{a}$ to $\bar{b}$.*

Proof. We iterate the following lemma:

Suppose M is an $\mathcal{L}$-structure, $A \subseteq M$ and $f : A \to M$ is a partial elementary map, i.e., $M \models \varphi(a_1, \ldots, a_n)$ iff $M \models \varphi(f(a_1), \ldots, f(a_n))$ for all $a_i \in A$. If $b \in M$, we can find an elementary extension N of M and extend f to a partial elementary map from $A \cup \{b\}$ into N. $\square$

Stone space

For each $\mathcal{L}_A$-formula $\varphi(x_1, \ldots, x_n)$, consider the set

$$B_\varphi = \{p \in S_n(A) \; : \; \varphi \in p\}.$$

The *Stone topology* on $S_n(A)$ is generated by the basic open sets B_φ.

Theorem 21. *The Stone space $S_n(A)$ is compact and totally disconnected.*

Proof. Note that $S_n(A) \setminus B_\varphi = B_{\neg\varphi}$ so each B_φ is open and closed. Thus $S_n(A)$ is totally disconnected.

Suppose $\{B_{\varphi_i} : i \in I\}$ is a cover of $S_n(A)$ by basic open sets. Then

$$\bigcap_i B_{\neg\varphi_i} = \emptyset,$$

and thus the set $\{\neg\varphi_i : i \in I\}$ is inconsistent. By Compactness, it has a finite inconsistent subset $\{\neg\varphi_i : i \in I_0\}$ and $\{B_{\varphi_i} : i \in I_0\}$ is a finite subcover. $\square$

Motivation for saturation

In the previous discussion of types, in order to find realisations, or to relate types to Galois considerations, we had to go to elementary extensions.

Sometimes it would be useful if we could do this without changing the model.

Saturation

Definition 22.

- Let κ be an infinite cardinal. We say that a structure M is κ-*saturated* if for every $A \subseteq M$ with $|A| < \kappa$, all the types in $S_1(A)$ are realised in M.
- We say that M is *saturated* if it is $|M|$-saturated.

An easy inductive argument shows that if M is κ-saturated and $|A| < \kappa$, then every type in $S_n(A)$ is realised in M^n.

Advantages of Saturation

Theorem 23. *Suppose M is saturated. Then:*

- *M is strongly homogeneous, i.e., if $A \subseteq M$ and $|A| < |M|$, then $tp(\bar{a}/A) = tp(\bar{b}/A)$ if and only if there is an automorphism of M fixing A and mapping $\bar{a}$ to $\bar{b}$.*
- *M is universal, i.e., every small model of $Th(M)$ embeds into M.*

Model-theorists usually fix a huge homogeneous and universal model of the theory they study, usually called the *monster model* and then consider any particular model as an elementary substructure of the monster.

Example: ACF and saturation

Theorem 24. *An algebraically closed field K is saturated if and only if it is of infinite transcendence degree.*

Proof. Suppose $A \subset K$ is finite and F is the field generated by A. Let p be the 1-type over A which says that x is transcendental over F. If K is $\aleph_0$-saturated, then p must be realised in K. Thus, we inductively conclude that an $\aleph_0$-saturated ACF must be of infinite transcendence degree.

Conversely, supose K has infinite transcendence degree and $F \subseteq K$ is a field generated by fewer than $|K|$ elements. Consider the ideal

$$I_p := \{f(x) \in F[x] : \text{“}f(x) = 0\text{”} \in p\}.$$

If $I_p = 0$, then p says that x is transcendental over F, and we can find a realisation in K. If $I_p \neq 0$, since $F[x]$ is a PID, I_p is generated by some $f(x)$ and any zero of f in K realises p. $\square$

Example: DLO and saturation

Countable dense linear orders without endpoints are $\aleph_0$-saturated.

Question: what is the minimum size for an $\aleph_1$-saturated model?

Problems finding saturated models

The upper bound for the number of types is

$$|S_n(A)| \leq 2^{|A|+|\mathcal{L}|+\aleph_0},$$

which is sometimes attained, so there are set-theoretic problems associated with finding saturated models.

Typically we need to assume GCH or the existence of inaccessible cardinals to be able to find them.

Saturated models exist unconditionally if the theory is *stable*, to be discussed later.

3 Applications in algebra

Quantifier elimination

Definition 25. We say that a theory T admits *quantifier elimination* if for every formula $\psi(\bar{x})$ there is a quantifier-free formula $\varphi(\bar{x})$ such that

$$T \models \forall \bar{x}\ (\psi(\bar{x}) \leftrightarrow \varphi(\bar{x})).$$

Example: QE for dense linear orders without endpoints

Theorem 26. *The theory of dense linear orders without endpoints has QE.*

Direct proof. Let us write $x \leq y$ as a shorthand for $(x < y) \vee (x = y)$.

After some thinking, one sees that every quantifier-free formula is a $\wedge, \vee$-combination of formulae of form $x \leq y$ and $x < y$.

Since $\exists x(\varphi \vee \psi)$ is equivalent to $(\exists x\varphi) \vee (\exists x\psi)$, it is enough to show how to eliminate the quantifier from:

$$\exists x \bigwedge_i (y_i < x) \wedge \bigwedge_j (y_j \leq x) \wedge \bigwedge_k (x \leq z_k) \wedge \bigwedge_l (x < z_l).$$

But this is clearly equivalent to:

$$\bigwedge_{i,k} (y_i < z_k) \wedge \bigwedge_{i,l} (y_i < z_l) \wedge \bigwedge_{j,l} (y_j < z_l) \wedge \bigwedge_{j,k} (y_j \leq z_k).$$

QE test

Theorem 27. *Assume the language $\mathcal{L}$ contains at least one constant symbol. Let T be an $\mathcal{L}$-theory and let $\varphi(\bar{x})$ be an $\mathcal{L}$-formula (we allow the possibility that φ is a sentence). TFAE:*

1. *There is a quantifier-free formula $\psi(\bar{x})$ such that*
$$T \models \forall \bar{x}\ (\varphi(\bar{x}) \leftrightarrow \psi(\bar{x})).$$
2. *If A and B are models of T and C a common substructure of A and B, then $A \models \varphi(\bar{a})$ if and only if $B \models \varphi(\bar{a})$ for all $\bar{a} \in C$.*

QE test proof

$1 \Rightarrow 2$: Trivial, since qf formulae are preserved under (substructure) embeddings.

$2 \Rightarrow 1$: If $T \models \forall \bar{x}\ \varphi(\bar{x})$, then $T \models \forall \bar{x}\ (\varphi(\bar{x}) \leftrightarrow c = c)$. If $T \models \forall \bar{x}\ \neg\varphi(\bar{x})$, then $T \models \forall \bar{x}\ (\varphi(\bar{x}) \leftrightarrow c \neq c)$. Thus WMA both $\varphi(\bar{x})$ and $\neg\varphi(\bar{x})$ are consistent with T.

Let $\Gamma(\bar{x}) = \{\psi(\bar{x}) : \psi$ is qf and $T \models \forall \bar{x}(\varphi(\bar{x}) \rightarrow \psi(\bar{x}))\}$. Let $\bar{d}$ be new constant symbols. We will show below that $T \cup \Gamma(\bar{d}) \models \varphi(\bar{d})$ (*). Thus, by compactness there are $\psi_1, \ldots, \psi_n \in \Gamma$ such that $T \models \forall \bar{x}(\bigwedge_i \psi_i(\bar{x}) \rightarrow \varphi(\bar{x}))$. By definition of Γ, we get $T \models \forall \bar{x}(\bigwedge_i \psi_i(\bar{x}) \leftrightarrow \varphi(\bar{x}))$ and $\bigwedge_i \psi_i(\bar{x})$ is qf.

It remains to prove (*).

QE test proof

Claim: $T \cup \Gamma(\bar{d}) \models \varphi(\bar{d})$.

If not, let $A \models T \cup \Gamma(\bar{d}) \cup \{\neg\varphi(\bar{d})\}$. Let C be the substructure of A generated by $\bar{d}$ (if φ is a sentence the constant symbol ensures C nonempty). Let $\mathrm{Diag}(C)$ be the set of all atomic and negated atomic formulas with parameters from C that are true in C. Let $\Sigma = T \cup \mathrm{Diag}(C) \cup \varphi(\bar{d})$. If Σ is inconsistent, since C is generated by $\bar{d}$, there are qf formulae $\psi_1(\bar{d}), \ldots, \psi_n(\bar{d}) \in \mathrm{Diag}(C)$ such that $T \models \forall \bar{x}(\bigwedge_i \psi_i(\bar{x}) \rightarrow \neg\varphi(\bar{x}))$. But then $T \models \forall \bar{x}(\varphi(\bar{x}) \rightarrow \bigvee_i \neg\psi_i(\bar{x}))$. So $\bigvee_i \neg\psi_i(\bar{x}) \in \Gamma$ and $C \models \bigvee_i \neg\psi_i(\bar{x})$, a contradiction. Thus Σ is consistent.

Let $B \models \Sigma$. Since $\mathrm{Diag}(C) \subseteq \Sigma$, C embeds in B. But, since $A \models \neg\varphi(\bar{d})$, $B \models \neg\varphi(\bar{d})$, a contradiction.

QE down to $\exists_1$

Lemma 28. *Suppose that for every qf-formula $\theta(x, \bar{y})$ there is a qf-formula $\psi(\bar{y})$ such that*

$$T \models \forall \bar{y}\ (\exists x \theta(x, \bar{y}) \leftrightarrow \psi(\bar{y})).$$

Then T has QE.

Proof of the lemma

Proof. By induction on complexity of φ. Everything is trivial if φ is qf.The induction step is straightforward when φ is a Boolean combination of formulae for which the QE works.If $\varphi(\bar{y}) \equiv \exists x \theta(x, \bar{y})$, by inductive hypothesis we first find the qf-formula $\psi_0(x, \bar{y})$ equivalent to $\theta(x, \bar{y})$, and then by assumption a qf-formula $\psi(\bar{y})$ equivalent to $\exists x \psi_0(x, \bar{y})$. Then clearly $\psi(\bar{y})$ is a qf-formula equivalent to $\varphi(\bar{y})$. $\square$

NB This means that it suffices to check the condition in the QE test for $\exists_1$-formulae.

QE for ACF

Theorem 29 (Tarski)**.** *The theory ACF has quantifier elimination.*

Algebraic geometers' restatement:

A *constructible* subset of a variety X is a Boolean combination of Zariski closed subsets (a finite union of locally closed sets).

Theorem 30 (Chevalley)**.** *Let $f : X \to Y$ be a morphism of finite type. The image of a constructible subset of X under f is constructible in Y.*

I couldn't find a historical reference as to which came first.

Proof of QE for ACF

Let F be a field and let K, L be algebraically closed extensions of F, and let $\bar{F}$ be the algebraic closure of F, viewed as a subfield of both K and L. Let $\varphi(x, \bar{y})$ be a qf-formula, $a \in K$, $\bar{b} \in F$ such that $K \models \varphi(a, \bar{b})$. We need to show $L \models \exists x \varphi(x, \bar{b})$.

There are polynomials $f_{ij}, g_{ij} \in F[x]$ such that $\varphi(x, \bar{b})$ is equivalent to

$$\bigvee_i \left(\bigwedge_j f_{ij}(x) = 0\ \wedge\ \bigwedge_j g_{ij}(x) \neq 0 \right).$$

Then $K \models \bigwedge_j f_{ij}(x) = 0\ \wedge\ \bigwedge_j g_{ij}(x) \neq 0$ for some i. If not all f_{ij} are identically zero for that i, then $a \in \bar{F} \subseteq L$ and we are done. O/w, since $\bigwedge_j g_{ij}(a) \neq 0$, all g_{ij} are nonzero polynomials and have finitely many roots in L, so we can easily find an element $d \in L$ which satisfies all inequations, so $L \models \varphi(d, \bar{b})$.

Some applications of QE for ACF

Corollary 31. *Let K be an ACF.*

1. *Any definable subset of K in one variable is either finite or cofinite (strong minimality).*

2. *Let $f : K \to K$ be a definable function. If K is of characteristic 0, there is a rational function $g \in K(x)$ such that $f(a) = g(a)$ for all but finitely many $a \in K$. If K is of characteristic p, there is a rational function g and $n \geq 0$ such that $f(x) = g(x)^{1/p^n}$.*

Proof. 1. Every definable set in 1 variable is a boolean combination of sets of the form $\{x : f(x) = 0\}$ for a polynomial f and such sets are finite.

2. A 'generic point' argument. Assume $\operatorname{char}(K) = 0$. Let L be a proper elementary extension of K and let $a \in L \setminus K$. If σ is any automorphism of L fixing $K(a)$, then $\sigma(f(a)) = f^{\sigma}(\sigma(a)) = f(a)$. We conclude $f(a) \in K(a)$ and thus there is a rational function $g \in K(x)$ such that $f(a) = g(a)$. Consider $\varphi(x) \equiv f(x) = g(x)$. By above, $\varphi(K)$ is either finite or cofinite. If it were of size N, since $K \preceq L$, $\varphi(L)$ would also be of size N, contradicting the fact that $a \in \varphi(L) \setminus \varphi(K)$. Thus $\varphi(K)$ must be cofinite. $\square$

Stone space for ACF vs Spec

Recall: for $p \in S_n(F)$, we defined $I_p := \{f \in F[x_1, \ldots, x_n] : f(x_1, \ldots, x_n) = 0 \in p\}$.

Theorem 32. *If K is algebraically closed and F a subfield of K, the map $p \mapsto I_p$ is a continuous bijection between $S_n(F)$ and $\operatorname{Spec}(F[x_1, \ldots, x_n])$.*

Proof. If $fg \in I_p$, then $f(\bar{x})g(\bar{x}) = 0 \in p$. Since p is complete, either $f(x) = 0 \in p$ or $g(x) = 0 \in p$, so I_p is prime.

If $\mathfrak{p}$ is a prime ideal, we can find a prime ideal $\mathfrak{p}_1$ in $K[\bar{x}]$ such that $\mathfrak{p}_1 \cap F[\bar{x}] = \mathfrak{p}$. Let K_1 be the algebraic closure of $K[\bar{x}]/\mathfrak{p}_1$ and let $a_i = x_i + \mathfrak{p}_1$. For $f \in K[\bar{x}]$, $f(\bar{a}) = 0$ if and only if $f \in \mathfrak{p}_1$ and thus $I_{\operatorname{tp}(\bar{a}/F)} = \mathfrak{p}$ so the map is surjective. By QE, if $p \neq q$, then $I_p \neq I_q$, so the map is injective. Continuity is obvious. $\square$

Real closed ordered fields

The theory of real closed ordered fields RCF:

- the usual axioms for ordered fields;
- $\forall x > 0\, \exists y\ \ y^2 = x$;
- axiom schema: for every odd n, take the axiom:

$$\forall y_0 \cdots \forall y_{n-1} \exists x\ \ x^n + y_{n-1}x^{n-1} + \cdots + y_0 = 0.$$

QE for RCF

Theorem 33. *The theory RCF has quantifier elimination in the language of ordered rings.*

Proof of QE for RCF

Use the QE test. Let F_0, F_1 be models of RCF and let R be a common substructure (an ordered domain). Let L be the real closure of the fraction field of R. WMA L is a substructure of F_0 and F_1. Suppose $\varphi(x, \bar{y})$ is qf, $\bar{b} \in R$, $a \in F_0$ and $F_0 \models \varphi(a, \bar{b})$. We need to show $F_1 \models \exists x\ \varphi(x, \bar{y})$, but it is enough to show $L \models \exists x\ \varphi(x, \bar{y})$. WMA there are polynomials $f_i, g_j \in R[x]$ such that $\varphi(x, \bar{b})$ is equivalent to

$$\bigwedge_i f_i(x) = 0 \ \wedge \ \bigwedge_j g_j(x) > 0.$$

if not all of f_i are zero, it follows that a is algebraic over R and thus in L and we are done. Thus WMA $\varphi(x, \bar{b}) \equiv \bigwedge_j g_j(x) > 0$. Since L is RCF, we can factor each g_j as a product of factors of form $(x - c)$ and $x^2 + bx + c$ with $b^2 - 4c < 0$. Linear factors change sign at c, quadratic factors do not change sign, so we are left with a (consistent) linear system of inequalities which can definitely be solved in L.

Completeness of RCF

Corollary 34. *RCF is complete and decidable.*

Proof. We can embed $\mathbb{Q}$ inside any RCF F. Given a sentence φ, find the equivalent qf-formula ψ, and we get $F \models \varphi$ iff $\mathbb{Q} \models \psi$. Thus, for any two RCF's F_1 and F_2, $F_1 \models \varphi$ iff $\mathbb{Q} \models \psi$ iff $F_2 \models \varphi$. Decidability is a direct consequence of completeness as discussed before. □

o-minimallity

Corollary 35. *A definable subset (in one variable) of a real closed field is a finite union of points and intervals.*

The above property is called *o-minimality*.

Proof. Definable sets in one variable are boolean combinations of $\{x : f(x) > 0\}$ which are finite unions of intervals. □

Model completeness

Definition 36. A theory T is *model complete* if whenever $M, N \models T$ and $M \subseteq N$, then in fact $M \preceq N$.

Theorem 37. *If T has quantifier elimination, then T is model complete.*

Proof. Let $M \subseteq N$ be models of T. Suppose $\varphi(\bar{x})$ is a formula and $\bar{a} \in M$. There is a qf formula $\psi(\bar{x})$ such that $T \models \forall \bar{x}\ (\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}))$. Since $\psi(\bar{x})$ is qf, $M \models \psi(\bar{a})$ iff $N \models \psi(\bar{a})$. Thus $M \models \varphi(\bar{a})$ iff $N \models \varphi(\bar{a})$. □

Model-completeness vs QE

A theory can be model complete without admitting QE. For example:

- $\mathrm{Th}(\mathbb{R})$ in the language of rings.
- Wilkie's example: in $\mathrm{Th}(\mathbb{R}, +, -, \cdot, <, \exp, 0, 1)$, cannot eliminate the quantifier from
$$y > 0 \wedge \exists w \, (wy = x \ \wedge \ z = y \exp(w)).$$

Nullstellensatz from model-completeness

Theorem 38 (Weak Nullstellensatz)**.** *Let F be an algebraically closed field and let $I \subseteq F[x_1, \ldots, x_n]$ be a prime ideal. Then there is $\bar{a} \in F^n$ such that $f(\bar{a}) = 0$ for all $f \in I$.*

Proof. Let K be the algebraic closure of the fraction field of $F[x_1, \ldots, x_n]/I$. If we denote $b_i = x_i + I$, then $f(b_1, \ldots, b_n) = 0$ for all $f \in I$. If $f_1, \ldots, f_m$ generate I, then
$$K \models \exists \bar{y} \bigwedge_i f_i(\bar{y}) = 0.$$

By model completeness, this sentence is already true in F. □

The full version $I(V(J)) = \sqrt{J}$ is easily obtained using the 'Rabinovich trick'.

Hilbert 17 from model-completeness

Theorem 39 (Artin)**.** *Let F be a real closed field. Suppose that $f \in F(x_1, \ldots, x_n)$ is such that $f(\bar{a}) \geq 0$ for all $\bar{a} \in F^n$. Then f is a sum of squares of rational functions.*

Proof. If not, we can extend the order of F to $F(x_1, \ldots, x_n)$ such that $f < 0$. Let K be the real closure of $F(x_1, \ldots, x_n)$ with this ordering. Then
$$K \models \exists \bar{y} \, f(\bar{y}) < 0,$$
since $K \models f(\bar{x}) < 0$. By model completeness, F satisfies the same sentence, which is a contradiction. □

4 Dimension, rank, stability

Standard assumptions

We consider a *complete* theory T in a *countable* language $\mathcal{L}$ with infinite models. We fix a large saturated model $\mathfrak{C}$.

Thus, any (small) model M of T is an elementary substructure of $\mathfrak{C}$.

Algebraic and definable closure

For $A \subseteq \mathfrak{C}$ (small), let

1. the *definable closure* of A be

$$\mathrm{dcl}(A) = \{c \in \mathfrak{C} : c \text{ is fixed by any automorphism of } \mathfrak{C} \text{ fixing } A\};$$

2. the *algebraic closure* of A be

$$\mathrm{acl}(A) = \{c \in \mathfrak{C} : c \text{ has finitely many conjugates over } A\};$$

Clearly, $c \in \mathrm{dcl}(A)$ iff $\{c\}$ is an A-definable set, and $c \in \mathrm{acl}(A)$ iff c is contained in a finite A-definable set.

Example 40. Let $A \subseteq \mathfrak{C} \models ACF$. Then $\mathrm{dcl}(A)$ is the perfect closure of the field generated by A, and $\mathrm{acl}(A)$ is the (usual) algebraic closure of the field generated by A.

Imaginaries

For each $\emptyset$-definable equivalence relation $E(\bar{x}, \bar{y})$ on $\mathfrak{C}^n$, we add a new sort with interpretation $\mathfrak{C}^n/E$ to the language, along with a new function symbol for the natural projection $\mathfrak{C}^n \to \mathfrak{C}^n/E$.

The resulting language is denoted $\mathcal{L}^{eq}$, the structure $\mathfrak{C}^{eq}$, and let T^{eq} be the theory of $\mathfrak{C}^{eq}$.

Why consider imaginaries?

The following are equivalent:

- T *eliminates imaginaries*, i.e., every element of $\mathfrak{C}^{eq}$ is interdefinable with a tuple from $\mathfrak{C}$;
- every definable set D has a *canonical parameter*, i.e., a tuple $\bar{c}$ such that $\bar{c}$ is fixed by exactly those automorphisms fixing D setwise.

Theorem 41. *T^{eq} eliminates imaginaries.*

Example 42. ACF eliminates imaginaries.

Morley rank

To each definable set X we wish to associate its $On \cup \{-1, \infty\}$-valued *Morley rank*:

Definition 43.
- $MR(X) \geq 0$ if X is not empty;
- $MR(X) \geq \lambda$ if $MR(X) \geq \alpha$ for all $\alpha < \lambda$ for a limit ordinal λ;
- $MR(X) \geq \alpha + 1$ if there is an infinite family X_i of disjoint definable subsets of X such that $MR(X_i) \geq \alpha$ for all i.

Then we set $MR(X) = \sup\{\alpha : MR(X) \geq \alpha\}$, with the convention $MR(\emptyset) = -1$ and $MR(X) = \infty$ if $MR(X) \geq \alpha$ for all ordinals α.

Definition 44. If $MR(X) = \alpha$, we let the *Morley degree* $Md(X)$ be the maximal length d of a decomposition $X = X_1 \sqcup \cdots \sqcup X_d$ into pieces of rank α.

Additivity of MR and Md

- If $X \subseteq Y$, then $MR(X) \leq MR(Y)$.
- $MR(X \cup Y) = \max\{MR(X), MR(Y)\}$.
- If X and Y are disjoint with $MR(X) \leq MR(Y)$, then

$$Md(X \cup Y) = \begin{cases} Md(X) + Md(Y), & \text{when MR(X)=MR(Y),} \\ Md(Y), & \text{otherwise.} \end{cases}$$

MR and Md of a type

For a type p which contains ranked formulae, pick a formula $\varphi \in p$ of minimal rank α, and of minimal degree among all the formulae of rank α in p. We then let $MR(p) = \alpha$, and $Md(p) = d$.

Such a φ *determines* p as the only type over A which contains it and has at least rank α.

Given a formula $\varphi \in \mathcal{L}(A)$, we have:

- $MR(\varphi) = \max\{MR(p) : p \in S(A), \varphi \in p\}$;
- $Md(\varphi) = \sum\{Md(p) : p \in S(A), \varphi \in p, MR(p) = MR(\varphi)\}$.

MR in ACF

In algebraically closed fields,

- $MR(X)$ equals the Krull dimension of the Zariski closure of X.
- For an algebraic set X, $Md(X)$ is the number of irreducible components of top dimension of X.

Totally transcendental theories and ω-stability

Definition 45.

- T is *totally transcendental* if every definable set has MR.
- T is *ω-stable* is for every countable A, $S_1(A)$ is countable.

Example 46. The theory of dense linear orders without endpoints is not ω-stable: there is a continuum of Dedekind cuts over $\mathbb{Q}$.

Totally transcendental vs ω-stable theories

Theorem 47. *A theory T is totally transcendental if and only if T is ω-stable.*

Proof. If T is totally transcendental, every type over A is determined by an $\mathcal{L}(A)$-formula, and so

$$S_1(A)| \leq |\mathcal{L}(A) - \text{formulae}| = |A| + \aleph_0.$$

Conversely, assume T is totally transcendental, and thus $MR(x = x) = \infty$. Starting from $X_\emptyset = \mathfrak{C}$, build a binary tree of definable subsets $(X_s : s \in {}^{<\omega}2)$ of infinite MR

such that $X_s \neq \emptyset$, $X_{si} \subset X_s$ for $i = 0, 1$, and $X_{s0} \cap X_{s1} = \emptyset$. Choose a countable set A containing parameters for all X_s, and it is clear that every path $\sigma \in {}^{\omega}2$ determines a type $p_\sigma \in S_1(A)$ which contains all X_s, for $s \subset \sigma$. The p_σ are all different so $S_1(A)$ has continuum many elements.

$\square$

Strongly minimal sets

Recall:

Definition 48. A definable set X is *strongly minimal* if it is infinite and every definable subset of X is either finite or cofinite.

Lemma 49. *X is strongly minimal iff $MR(X) = 1$ and $Md(X) = 1$.*

The same definition applies for types.

Pregeometries

Definition 50. A *pregeometry* (A, cl) is a set A together with a closure operator $cl : \mathbb{P}(A) \to \mathbb{P}(A)$ such that:

- for any $B \subseteq A$, $B \subseteq cl(B) = cl(cl(B))$,
- if $B \subseteq C \subseteq A$ then $cl(B) \subseteq cl(C)$,
- if $B \subseteq A$ and $b \in cl(B)$ there is a finite $B_0 \subseteq B$ such that $b \in cl(B_0)$, and
- (Steinitz exchange) if $B \subseteq A$, $b \in cl(B \cup \{c\}) \setminus cl(B)$ then $c \in cl(B \cup \{b\})$.

Definition 51. If (A, cl) is a pregeometry, we say that $B \subseteq A$ is *independent* if $b \notin cl(B\ b)$ for any $b \in B$. A *basis* for a set C is an independent set $B \subseteq C$ such that $C \subseteq cl(B)$.

Examples of pregeometries

Example 52.
- A vector space with the linear span as closure.
- An affine space with the affine span.
- A field with the (relative) algebraic closure.

Dimension in pregeometries

Theorem 53. *Suppose (A, cl) is a pregeometry . Then, for any $B \subseteq A$, any maximal independent subset of B is a basis for B. Moreover, any two bases for B have the same cardinality.*

Proved exactly the same way as for vector spaces.

Algebraic closure in definable sets

Definition 54. Let X be a definable set with parameters $\bar{d}$. For $Y \subseteq X$, let

$$\mathrm{acl}_X(Y) = \mathrm{acl}(Y \cup \{\bar{d}\}) \cap X.$$

Theorem 55. *If X is strongly minimal, then (X, acl_X) is a pregeometry.*

Morley's Theorem

Theorem 56 (Morley)**.** *If T is categorical in some uncountable cardinal, it is categorical in all uncountable cardinals.*

We will mention some results used in the proof. Suppose T is categorical in an uncountable cardinality. Then:

1. T is ω-stable.
2. T has a prime model.
3. T has a strongly minimal formula $\varphi(x)$ over the prime model.
4. If M and N are models of T of the same uncountable cardinality, there is a partial elementary bijection between $\varphi(M)$ and $\varphi(N)$ (think of bases).
5. We extend this to an isomorphism $M \cong N$.

Number of models in countable cardinality

Theorem 57 (Baldwin-Lachlan)**.** *If T is uncountably categorical but not $\aleph_0$-categorical, then T has exactly $\aleph_0$ non-isomorphic models of size $\aleph_0$.*

Quantity vs quality

The theorems of Morley and Baldwin-Lachlan give information about the number of isomorphism types of models of given size, which is a form of classification, but they do not allow a qualitative classification. In that direction, there is a stream of results which allow us, under certain model-theoretic assumption, to identify a classical (algebraic or combinatorial) structure present. For example:

Theorem 58 (Macintyre)**.** *An infinite ω-stable field is algebraically closed.*

Let us work toward the sketch of proof.

Forking

We work in an ω-stable T.

Definition 59. Let $A \subseteq B$, p a type over A and q a type over B which extends p. We say that q is a *nonforking* extension of p if $MR(p) = MR(q)$.

It is convenient to use the notation $a \perp_B b$ to express that $tp(a/Bb)$ is a nonforking extension of $tp(a/B)$ (read as "a is independent from b over B").

Properties of nonforking/independence

inv $\mathop{\smile\!\!\!\!\!\!\,|}$ is invariant under automorphisms of $\mathfrak{C}$;

fc if for all finite tuples $a \in A$, $b \in B$, $a \mathop{\smile\!\!\!\!\!\!\,|}_E b$, then $A \mathop{\smile\!\!\!\!\!\!\,|}_E B$;

mon1 $A \mathop{\smile\!\!\!\!\!\!\,|}_E B$ and $B \supseteq D$ implies $A \mathop{\smile\!\!\!\!\!\!\,|}_E D$;

mon2 $A \mathop{\smile\!\!\!\!\!\!\,|}_E B$ and $B \supseteq D \supseteq E$ implies $A \mathop{\smile\!\!\!\!\!\!\,|}_D B$;

trans $A \mathop{\smile\!\!\!\!\!\!\,|}_E D$, $A \mathop{\smile\!\!\!\!\!\!\,|}_D B$ for $B \supseteq D \supseteq E$ implies $A \mathop{\smile\!\!\!\!\!\!\,|}_E B$;

symm $A \mathop{\smile\!\!\!\!\!\!\,|}_E B$ if and only if $B \mathop{\smile\!\!\!\!\!\!\,|}_E A$;

ex for all A, B, there is A' with $tp(A'/E) = tp(A/E)$ and $A' \mathop{\smile\!\!\!\!\!\!\,|}_E B$;

lc for every finite tuple a and all B, there is $E \subseteq B$ with $|E| \leq |T|$ such that $a \mathop{\smile\!\!\!\!\!\!\,|}_E B$.

Stationarity

Another property, slightly different in character from the others:

stat A type $tp(a/M)$ over a model M is *stationary*, i.e., has a unique nonforking extension to any $B \supseteq M$.

Also works if the type is over a set A such that $A = \mathrm{acl}^{eq}(A)$.

Proof of Macintyre's theorem

Sketch of proof:

Let F be an infinite ω-stable field, and let K be its algebraic closure. Using just general results about groups definable in ω-stable theories, one shows that F is perfect.

Claim: if $a_0, \dots, a_{n-1}$ are generic independent in F (i.e., for every i, $a_i \mathop{\smile\!\!\!\!\!\!\,|} a_0, \dots, a_{i-1}, a_{i+1}, \dots a_{n-1}$), then all solutions of $X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$ in K are already in F (*).

Proof of the Claim: Let $b_0, \dots, b_{n-1}$ be generic independent in F (over $\emptyset$). Let $c_0, \dots, c_{n-1}$ be the symmetric functions in $b_0, \dots, b_{n-1}$. Then the b_i are the roots of $X^n + c_{n-1}X^{n-1} + \dots + c_1 X + c_0$. The $c_i \in F$, and $b_0, \dots, b_{n-1} \in \mathrm{acl}(c_0, \dots, c_{n-1})$ in F. Thus $c_0, \dots, c_{n-1}$ are independent generic elements of F over $\emptyset$. Uniqueness of the generic type of F implies that $tp(a_0, \dots, a_{n-1}) = tp(c_0, \dots, c_{n-1})$. Thus by automorphism (*) has n distinct solutions in F, proving the claim.

Now let $P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$ be the minimal polynomial of some element $\alpha \in K$. Assume for a contradiction that $\alpha \notin F$, namely $n > 1$. As F is perfect P has distinct roots $\{\alpha_1, \dots, \alpha_n\}$. So $L = F(\alpha_1, \dots, \alpha_n)$ is a Galois extension of F, and moreover the $n \times n$ Vandermonde matrix whose i-th row is $[1, \alpha_i, \alpha_i^2, ..., \alpha_i^{n-1}]$ is invertible. Let $t_0, \dots, t_{n-1} \in F$ be generic independent over $\{a_0, \dots, a_{n-1}\}$, and let (**) $r_i = t_0 + t_1\alpha_i + t_2\alpha_i^2 + \dots + t_{n-1}\alpha_i^{n-1}$. Let $c_0, ..., c_{n-1}$ be the elementary symmetric functions in $r_1, \dots, r_n$. Then (as each c_i is fixed by $Gal(L/F)$), the c_i are in F. Now we have

(iii) each t_i is in the field generated by $\alpha_1, \dots, \alpha_n, r_1, \dots, r_n$.

(iv) (working in L) each r_i is field-theoretically algebraic over $\{c_0, \ldots, c_{n-1}\}$. It follows from (iii) and (iv) that in F, for each i

(v) $t_i \in \operatorname{acl}(a_0, \ldots, a_{n-1}, c_0, \ldots, c_{n-1})$.

We deduce again that $c_0, \ldots, c_{n-1}$ are generic, independent (over $\emptyset$) elements of F. By (ii), $r_1, \ldots, r_n$ are in F. But then (**) contradicts the fact that the minimal polynomial of α over F has degree n. Thus $\alpha \in F$. We have shown that F is algebraically closed.

Stability

Definition 60.

- T is λ-stable if $|A| \leq \lambda$ implies $|S_1(A)| \leq \lambda$.
- T is *stable* if it is λ-stable for some λ.
- T is *superstable* if it is λ-stable for all sufficiently large λ.

Definition 61. A formula $\varphi(\bar{x}, \bar{y})$ has the *order property* if there are tuples $\bar{a}_i, \bar{b}_i$, $i < \omega$ such that

$$\models \varphi(\bar{a}_i, \bar{b}_j) \text{ if and only if } i \leq j.$$

Stability and order

Theorem 62. *T is stable if and only if there is no formula with the order property.*

Example 63. Thus, the following are clearly unstable:

- the theory of dense linear orders without endpoints;
- RCF (even $Th(\mathbb{R}, +, \cdot, 0, 1)$).

5 Classification theory

Categoricity spectrum of a theory

Definition 64. Let T be a complete theory. We write $I(T, \lambda)$ for the number of models of T of cardinality λ up to isomorphism.

Morley's Theorem can be rephrased in this language:

Theorem 65. *For countable T, if $I(T, \lambda) = 1$ for some uncountable λ, then $I(T, \mu) = 1$ for all uncountable μ.*

From Morley to Classification

Morley conjectured that for a countable T, $I(T, \cdot)$ is monotonous on uncountable cardinals, i.e. $\aleph_0 < \lambda \leq \mu$ implies $I(T, \lambda) \leq I(T, \mu)$.

Shelah devoted 15 years to completely resolving all aspects of this problem, including determining the possibilities for the categoricity spectrum and classifying theories according to whether they have a *structure* or a *non-structure* theory.

Shelah's Classification

Theorem 66 (The Main Theorem)**.** *For every countable T, either $I(T, \lambda) = 2^\lambda$ for every uncountable λ, or $I(T, \aleph_\alpha) < \beth_{\omega_1}(|\alpha|)$ and every model of T can be characterized up to isomorphism by an invariant of countable depth.*

Recall,

$$\beth_\beta(\mu) = \mu + \sum_{\gamma<\beta} 2^{\beth_\gamma(\mu)}.$$

Shelah's Classification

The Classification Problem. Classify the T's in a useful way, i.e., such that for suitable questions on the class of models of T the partition to cases according to the classification will be helpful.

Shelah gives a complete solution in terms of dichotomy theorems associated with (not) having one of the five model theoretic properties: being *stable, superstable*, having *dop, deep, otop*. The one we can state here:

Theorem 67. *If T is not superstable, for uncountable λ, $I(T, \lambda) = 2^\lambda$.*

Thus, only a superstable T has a hope of having a 'structure theory'.

Shelah's Classification

- Morley's conjecture readily follows from Shelah's theory.
- Shelah proceeds to study the classification for uncountable T and for 'abstract elementary classes'.

This is a complete *quantitative* classification of first order theories, but it does not give much in terms of a *qualitative* description of structures.

6 Geometric model theory

Zilber's Trichotomy

A model of an uncountably categorical theory must (essentially) be either:

- trivial (such as a set with no structure);
- a vector space;
- an algebraically closed field.

In order to identify which, one must consider the types of pregeometries arising on strongly minimal sets.

Types of pregeometries

Definition 68. A pregeometry (X, cl) is:

- *trivial*, if $cl(A) = \cup_{a \in A} cl(\{a\})$ for all $A \subseteq X$;
- *modular*, if whenever $A, B \subseteq X$ are finite dimensional,

$$\dim(A) + \dim(B) = \dim(A \cup B) + \dim(A \cap B);$$

- *locally modular* if the above holds whenever $A \cap B \neq \emptyset$.

Thus, Zilber's principle would entail that a non-locally modular strongly minimal set 'interprets' an algebraically closed field.

In a similar direction, a conjecture of Cherlin and Zilber states that an infinite simple group of finite Morley rank must be an algebraic group over an algebraically closed field.

Types of pregeometries

Some (qualitative) classification results:

Theorem 69 (Cherlin-Harrington-Lachlan, Zilber)**.** *An ω-categorical strongly minimal set is locally modular.*

Theorem 70. *An ω-categorical strictly minimal set (where $cl(a) = \{a\}$ for all $a \in X$) is either a pure set, or a projective or affine geometry over a finite field.*

Zariski geometries

Using a sophisticated variant of Fraïssé amalgamation, Hrushovski refuted Zilber's conjecture in full generality by producing a non-locally modular strongly minimal set which does not even interpret a group.

Hrushovski and Zilber then prove that under the assumption on the existence of a certain topology on a structure (reminiscent of the Zariski topology), Zilber's trichotomy holds. They dub such structures *Zariski geometries*.

Cherlin-Zilber?

The Cherlin-Zilber conjecture is still open, even though many cases have been dealt with and it is now widely believed to be true.

The methods are similar to the ones employed in the classification of finite simple groups through the analogy of 'finite' and 'finite rank'.

Hrushovski's proofs of Mordell-Lang and Manin-Mumford

Some of the most spectacular applications of model theory in Diophantine geometry came through Hrushovski's proofs of Mordell-Lang and Manin-Mumford conjectures.

We recall some of the background necessary for understanding the ideas involved.

Abelian varieties

Definition 71. An *abelian variety* is a connected complete algebraic group.

Example 72. The elliptic curve given by the equation $zy^2 = x^3 + axz^2 + bz^3$ in $\mathbb{P}^2$, where $4a^3 + 27b^2 \neq 0$. (explain addition).

Theorem 73. *Let A be an abelian variety over and ACF k.*

- *A is commutative.*
- *A is divisible.*
- *torsion points are dense and in char 0 we get: $A_{torsion} = (\mathbb{Q}/\mathbb{Z})^{2g}$. More precisely, if $l \neq char(k)$, $\ker[l^n] = (\mathbb{Z}/l^n\mathbb{Z})^{2g}$.*

Jacobian of a curve

Each smooth and projective curve X of genus $g \geq 1$ can be embedded in its *Jacobian variety* $J(X)$ which is an abelian variety of dimension g classifying degree zero divisors up to rational equivalence.

Namely, if P_0 is a point on X, the embedding $X \to J(X)$ can be thought of as $P \mapsto [P] - [P_0]$.

NB. For an elliptic curve E, $J(E) \cong E$.

Semi-abelian varieties

Theorem 74 (Chevalley)**.** *Let G be a connected algebraic group and L the maximal connected affine subgroup of G. Then G/L is an abelian variety.*

Definition 75. A *semi-abelian variety* is a commutative algebraic group G which is an extension of an abelian variety A by a torus $T = \mathbb{G}_m^r$ as in the following short exact sequence:

$$0 \to T \to G \to A \to 0.$$

Beginnings of Diophantine geometry

Theorem 76. *Let X be a smooth and projective curve over $\mathbb{Q}$. Then:*

- *If X is of genus 0, then either $X(\mathbb{Q}) = \emptyset$ (e.g., $x^2+y^2+1=0$) or all but finitely many solutions are parametrised by rational fractions (e.g., all solutions of $x^2 + y^2 - 1 = 0$ except $(0,1)$ are parametrised by $(2t/(t^2+1), (t^2-1)/(t^2+1))$).*
- *If X is of genus 1, then either $X(\mathbb{Q}) =$ or X is an elliptic curve, so Mordell-Weil Theorem states that $X(\mathbb{Q})$ is a finitely generated group. More generally, for an abelian variety A and K a number field, $A(K)$ is finitely generated.*
- *If X is of genus ≥ 2, then Faltings' Theorem (originally Mordell conjecture) states that $X(\mathbb{Q})$ is finite.*

Lang's conjecture for curves

Combining the above results, by observing X in its Jacobian $A = J(X)$, one can come up with the following restatement of Mordell's conjecture:

> Let X be a curve in an abelian variety A and let Γ be a finitely generated subgroup of A. Then, $X \cap \Gamma$ is finite, except when X is a translate of an elliptic curve.

In the direction of Manin-Mumford conjecture:

> Let X be a curve in an abelian variety A. Then $X \cap A_{\text{torsion}}$ is finite, except when X is a translate of an elliptic curve.

Lang's conjecture

Lang's conjecture for curves

Let X be a complex curve in an abelian variety A and let Γ be a subgroup of finite rank (in the divisible hull of a f.g. subgroup) in A. Then $X \cap \Gamma$ is finite, except when X is a translate of an elliptic curve.

Lang's conjecture absolute form char 0

Let X be a subvariety of an abelian variety A over ACF K of char 0 and let Γ be a subgroup of finite rank in A. Then there exist $\gamma_1, \dots, \gamma_m \in \Gamma$ and $B_1, \dots, B_m$ abelian subvarieties such that $\gamma_i + B_i \subseteq X$ and

$$X(K) \cap \Gamma = \bigcup_{i=1}^{n} \gamma_i + (B_i(K) \cap \Gamma).$$

Diophantine equations over function fields

If K_0 is an algebraically closed field, a *function field* K over K_0 (of transcendence degree 1) is the field of rational functions of a variety (of dimension 1) over K_0.

Now the natural question to ask is not whether $X(K)$ is finite, but possibly whether $X(K) \setminus X(K_0)$ finite.

Example 77. Let X be the Fermat curve defined by $X^n + Y^n = Z^n$ for some $n \geq 3$. Then $X(\mathbb{C}(T)) \setminus X(\mathbb{C}) = \emptyset$.

Mordell for function fields

Theorem 78 (Mordell's conjecture over function fields)**.** *Let X be a curve of genus ≥ 2 defined over K which is a function field over K_0. Then $X(K)$ is finite unless X is isotrivial, i.e., there is a curve X_0 defined over K_0 and isomorphic to X over some finite extension K' of K.*

There is also a relative Mordell-Weil theorem, but we do not state it here.

Relative Lang's conjecture

Lang's conjecture over function fields
Let K be a function field over an ACF K_0, let X be a subvariety of an abelian variety A both defined over K. Assume $Stab_X$ is finite. Let Γ be a subgroup of A of finite rank, defined over the algebraic closure of K. Then either $X \cap \Gamma$ is not Zariski dense in X or there is a bijective morphism $X \to X_0$ onto a variety X_0 defined over K_0.

Model-theoretic content

Definition 79. Let K be an algebraically closed field and A a commutative algebraic group over K (which we identify with its set of K-rational points) and let Γ be a subgroup of A. We say that the triple (K, A, Γ) is of *Lang-type* if for every n and every subvariety X (over K) of A^n, $X \cap \Gamma^n$ is a finite union of cosets.

Remark
Lang's conjecture says that if Γ is a finite rank subgroup of a semi-abelian variety A over $\mathbb{C}$, then $(\mathbb{C}, A, \Gamma)$ is of Lang-type.

One-based stable groups

Theorem 80 (Hrushovski-Pillay). *Let T be a stable theory, M a big model of T and G an $\emptyset$-definable group in M. Then G is one-based in T (a property generalising modularity mentioned before in the strongly minimal setting) if and only if every definable (with parameters) subset of G^n is a finite Boolean combination of cosets (of definable subgroups of G^n).*

Theorem 81. *(K, A, Γ) is of Lang-type if and only if $Th(K, +, \cdot, \Gamma, a)_{a \in K}$ is stable and the formula "$x \in \Gamma$" is one-based.*

Proof of ML function field case all characteristics
We have $K_0 \subseteq K$ two distinct algebraically closed fields A an abelian variety defined over K, X a subvariety of A defined over K and Γ a subgroup of finite rank of $A(K)$. The aim is to show that either:

1. $X \cap \Gamma$ is a finite union of cosets of subgroups of Γ, or
2. the situation 'descends' to K_0.

In model-theoretic terms, we would like to show 1. by showing that $Th(K, +, \cdot, \Gamma, a)_{a \in K}$ is stable and Γ is one-based, but the problem is that Γ is not definable in any natural sense of the word.

Proof of ML function field case all characteristics
Thus we must replace Γ by a *definable* object which is small enough (finite rank) so that the conclusion will still hold. The language of rings is too coarse, we must expand the language:

1. in char 0, we replace Γ by a definable group of finite Morley rank in the language of *differential fields* (we add a symbol for the derivation such that K_0 is contained in the constants).

2. in char p, we replace K by a *separably closed* but not algebraically closed field K such that $K_0 = K^{p^\infty}$ and use the fact that the definable sets are much finer than just constructible sets; Γ is replaced by a type-definable object of finite U-rank.

3. in the proof of Manin-Mumford the torsion is expressed using the language of *difference fields* (fields with a symbol for an automorphism), so that K_0 contains the fixed field. These are not stable, but are *simple*, i.e. still have a good theory of forking and some local ranks.

The proof continues via model-theoretic analysis of one-basedness in the above theories. One proves that a non-one-based set must be 'closely tied' to:

- the field of constants in case 1;
- the field K^{p^∞} in case 2;
- the fixed field in case 3.

Isotriviality follows.

Model Theory and Mathematics

- I hope I managed to convince you that Model Theory provides an important alternative point of view to the classical methods in many mainstream areas of Pure Mathematics.
- Moreover, model-theorists are more easily convinced to abandon the strict confines of the classical methods and develop a more general 'geometry', for example in difference or differential fields, and thus may be able to reach further than others in some directions.

Literature

1 E. Bouscaren (Ed.) **Model Theory and Algebraic Geometry. (An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture).** Lecture Notes in Mathematics **1696,** Springer, 1998.

2 C. C. Chang and H. J. Keisler. **Model Theory.** Studies in Logic and the Foundations of Math. **73,** North-Holland Publishing Co., Amsterdam, 1990.

3 D. Haskell, A. Pillay, C. Steinhorn (Eds.). **Model Theory, Algebra, and Geometry.** MSRI Publications, Volume **39,** 2000.

4 W. Hodges, **Model Theory.** Encyclopedia of Mathematics and its Applications **42,** Cambridge University Press, Cambridge, 1993.

Comments on literature

The first part of the notes closely follows D. Marker's contribution from 3, and the material on the Mordell-Lang conjecture is from 1.